UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,457	12/19/2000	Chin-Long Chen	POU920000179US1	4045

7590 01/19/2005

Lawrence D. Cutter, Attorney
IBM Corporation
Intellectual Property Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/740,457	CHEN ET AL.	
	Examiner	Art Unit	
	Zachary A Davis	2137	

-- The MAILING DATE of this c mmunication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. An amendment was received on 23 August 2004. Claims 1-4 and 6 have been amended. No claims have been added or canceled. Claims 1-6 are currently pending in the present application.

Specification

2. The objection to the specification for informalities is maintained. Although Applicant has corrected errors in the specification, Applicant has not addressed the specific errors referred to in the previous Office action.

Response to Arguments

3. Applicant's arguments filed 23 August 2004 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 1 and 2 under 35 U.S.C. 102(b) as being anticipated by Tenca and Koc, "A Scalable Architecture for Montgomery Multiplication", hereinafter "Tenca", Applicant argues that Tenca is directed to multiplication operations, whereas Claims 1 and 2 of the present application are directed to determining *A* mod *N* and do not mention Montgomery Multiplication. First, the Examiner believes that Tenca does disclose determining *A* mod *N* (see page 96, where the integer value of *a*, or

a mod *M* is determined). Second, although Montgomery Multiplication is not explicitly named in the claims, the Examiner respectfully draws Applicant's attention to, for example, page 96 of Tenca, where Montgomery Multiplication is defined as an operation of the form XYr^{-1} mod *M*. Applicant's "calculating engine" produces similar output, where $X=x$, $Y=y$, $r=2^{mk}$, and $M=N$.

Applicant further argues that the claims are directed to processing multi-bit word segments and that Tenca does not teach blocking of variables into *m* words having *k* bits each, and that Tenca specifically teaches against such processing. The Examiner respectfully disagrees. In a section cited by Applicant, Tenca states that, "the operand *Y* (multiplicand) is scanned word-by-word" (page 97). The Examiner therefore believes that Tenca does indeed teach blocking variables into words, and does not specifically teach against that. Additionally, Applicant alleges that, "in Tenca, the term 'word' refers to the entire variable *A* not to *k* bit chunks which are processable by a calculating engine". However, Applicant does not provide a citation in support of that allegation; the Examiner believes that Tenca's "words" are indeed fixed-length chunks that can be processed (see page 97, where *M* and *Y* are divided into "vectors" where "the words are marked by superscripts").

Regarding the rejection of Claim 3 under 35 U.S.C. 102(a) as being anticipated by Compaq Computer Corporation, "Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment", hereinafter "Compaq", Applicant agrees with the Examiner's previous mapping of variables from Compaq to Claim 3 of the present application. Applicant argues that the results produced, namely:

$$(((A_{pB} - (A_{qB} \bmod N_p))\ (N_q^{-1} \bmod N_p)) \bmod N_p)\ N_q + A_{qB}$$

resulting from Compaq, and:

$$N_q\ ((A_{pB} - A_{qB}) \bmod N_p)\ (N_q^{-1} \bmod N_p) \bmod N_p + A_{qB}$$

resulting from Applicant's claim, are not identical. It appears that Applicant refers to the location of the term N_q and the placement of parentheses. The Examiner would like to bring Applicant's attention to the fact that modular multiplication obeys the commutative property, and therefore whether the N_q term is pre-multiplied or post-multiplied does not affect the result of the calculation. Further, the Examiner brings Applicant's attention to the fact that modular arithmetic obeys the associative property, and therefore, as long as the order of operations is not changed by the grouping symbols, the placement of parentheses also does not affect the result of the calculation. Therefore, although the two results are written differently, they are equivalent mathematical expressions and therefore satisfy the requirements of 35 U.S.C. 102.

Regarding the rejection of Claims 4-6 under 35 U.S.C. 103(a) as being unpatentable over Compaq in view of Tenca, Applicant argues that Tenca teaches away from the use of "block structures" in processing. This argument has been addressed above in reference to Claims 1 and 2. Applicant further repeats the allegation that Tenca refers to words as the entire representation of variables, but does not provide a citation to support this allegation, as addressed in reference to Claims 1 and 2.

Therefore, in view of the above arguments, the Examiner maintains the rejections set forth below.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1 and 2 are rejected under 35 U.S.C. 102(b) as being anticipated by Tenca.

In reference to Claim 1, Tenca discloses a method for determining A mod N as the Montgomery reduction of A (page 96, noting especially that $\bar{a} = a\ r^2\ r^{-1}$ mod M is the modular reduction of a mod M) including a calculating engine that produces an output $x\ y\ 2^{-mk}$ mod N (page 96, equation 1, noting that r is a power of 2).

Claim 2 is an apparatus claim corresponding substantially to the method of claim 1, and is rejected by a similar rationale.

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claim 3 is rejected under 35 U.S.C. 102(a) as being anticipated by Compaq.

Compaq discloses a method for determining A^B mod N where N is the product of two prime numbers N_p and N_q including determining $A_p = A$ mod N_p, $A_q = A$ mod N_q,

$B_p = B \bmod (N_p - 1)$, $B_q = B \bmod (N_q - 1)$, $A_{pB} = (A_p)^{Bp} \bmod N_p$, $A_{qB} = (A_q)^{Bq} \bmod N_p$, and A^B (page 5, Figure 1, where $C=A$, $d=B$, $p=N_p$, $q=N_q$, $M=A^B$, $d_p=B_p$, $d_q=B_q$, $M_p=A_{pB}$, $M_q=A_{qB}$, and $u=U$).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Compaq in view of Tenca.

In reference to Claims 4 and 5, Compaq discloses everything as applied to Claim 3 above. However, Compaq does not explicitly disclose using an engine with output $x\, y^{-mk} \bmod N$ in the steps of determining the modular reductions.

Tenca discloses determining a modular reduction using a calculating engine that produces an output $x\, y\, 2^{-mk} \bmod N$ (page 96, equation 1, noting that r is a power of 2). Tenca also specifically discloses that these reductions are advantageous in modular exponentiation (page 96).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Compaq to use an engine with the given output in order to replace the division by N operation by a division by a power of 2

operation (see Tenca, page 94, paragraph 1) and to allow for fast and inexpensive modular multiplication for use in modular exponentiation (see Tenca, page 95, paragraph 1).

Claim 6 is an apparatus claim corresponding substantially to the method of claims 3-5, and is rejected by a similar rationale.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A Davis whose telephone number is (571) 272-

3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Caldwell

zad

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER